

## CITY OF SAN ANTONIO



### Administrative Directive

### AD 7.8E User Account Management

### Procedural Guidelines

Guidelines for managing user access to City IT resources.

### Department/Division

Information Technology Services Department (ITSD)

### Effective Date

July 6, 2009

### Project Manager

John Byers, Chief Information Security Officer (CISO)

## Purpose

User account management ensures that users have the access they need to information and information technology (IT) resources. To ensure that accounts and permissions are responsibly managed for as long as they are needed user access permissions should keep pace with user needs. Unmanaged access privileges can significantly contribute to breaches in the confidentiality, integrity, or availability of City of San Antonio (COSA) IT resources.

## Policy

This directive provides direction on managing user access to COSA and IT resources. This is a companion document to *7.8D Account Access Management* and other security related directives.

## Policy Applies To

☐ External & Internal Applicants

☒ Current Temporary Employees

☒ Current Full-Time Employees

☐ Current Volunteers

☒ Current Part-Time Employees

☒ Current Grant-Funded Employees

☒ Current Paid and Unpaid Interns

☒ Police and Fire Academy Trainees

☒ Uniformed Employees Under Collective Bargaining Agreements

## Definitions

N/A

## Policy Guidelines

### A. Access Authorization

1. All access to COSA information and IT resources must be authorized. Authorization shall be granted by business or system owners who are specifically delegated to perform this duty.
2. Access responsibility rests with the business or system owners.
3. For a system or application owned by ITSD, the Chief Information Officer (CIO), the Chief Technology Officer (CTO), or the person delegated to authorize access shall perform this duty. Authorizations must include the scope of authorized access based on the principles of:
  - a. Least-Privilege
    1. Individuals are only given access to the minimum necessary resources they need to perform the duties associated with their position at COSA.
  - b. Default Deny
    1. All activities are denied unless explicitly permitted.

### B. User Registration

1. Users shall be registered during their hiring and on-boarding process with the City. The process will begin with a positive verification of the user's identity and access requirements and end with the creation of a user account and the user acknowledging an understanding of his/her responsibilities relative to the account. The COSA Chief Information Security Officer (CISO) or their delegates shall have oversight of the registration processes that are performed.
2. All persons requesting access to COSA information and IT resources shall be positively identified. The processes established for the hiring of an individual or the processes used for an identification of contractor, vendor or third party is acceptable for these purposes. Authorized users shall have a unique UserID that they shall use to identify themselves to an IT resource.
3. Authorized users shall be assigned or required to create a unique password that is used to validate the authenticity of the UserID. Passwords shall comply with COSA *AD 7.6 Security and Passwords*.
4. Prior to granting access, users shall be trained by their respective department on their information security responsibilities and must formally acknowledge that they

## General Guidelines



understand their responsibilities. Further requirements are the acknowledgment of COSA *AD 7.4, Acceptable Use of Electronic Communication* and *AD 7.5 Acceptable Use of Information Technology*.

#### C. Administrator Registration

1. Registration of personnel with system administrator privileges shall follow a more rigorous approval process than the normal approval process. COSA *AD 4.55 Criminal Background Checks for Employment* provides additional information. Background checks shall be conducted in accordance with the standard and accepted practices for Security-sensitive Positions and Officers and relevant Federal, State, and local guidelines.
2. All system administrator actions shall be audited internally at least once a year. These reviews will be documented and may be conducted by senior IT management, IT security staff, and internal auditors. This review may also be conducted by external auditors or during a vulnerability assessment, which would be conducted either by a private company or by the Department of Homeland Security (DHS), or by the State of Texas Department of Information Resources (DIR).

#### D. Account Management

1. Business or system owners shall identify personnel who shall have access to the system in which they are owners. Business or system owners shall identify the data that the systems maintain, store, or process. This information will assist the system administrator in determining who shall be granted access.

#### E. Privilege Management

1. Access privileges to information and IT resources shall be reviewed on a regular basis depending on the type of system to ensure that users have the least privileges they need to fulfill their duties. The documented review shall be conducted under the guidance of the COSA IT CISO. To the extent possible, privileges should be role-based to reduce the complexity of administration and the possibility of introducing an unnecessary risk into the access management process.

#### F. Password Management

1. Passwords are the first technical line of defense against unauthorized users, COSA systems and/or application(s) shall have provisions for password management that complies with the requirements established in *AD 7.6 Security and Passwords*.

#### G. Account Termination

1. COSA systems and/or applications shall include provisions for the timely termination of accounts. The process shall ensure that administrators who are tasked with terminating accounts are informed when users leave, transfer, or no longer need their access privileges. The process shall also have provisions for account suspension or account locks during periods of inactivity. Responsibility rests with business or system owners to develop all processes. The process should be in accordance with direction from the Audit department and whether the system must comply with Federal, State, or local laws/ordinance.
2. Administrators shall periodically review the accounts as defined by the business or system owner, although no less than annually, for which they are responsible against lists/rosters of possible users.

#### H. Emergency Access

1. COSA user account provisioning process shall include access procedures to grant access privileges quickly and responsibly to those who need them during an emergency, such as the unavailability of a critical system.

#### I. Communication and Training Statement

1. All users of IT resources shall receive training regarding their responsibilities for complying with this directive. This directive shall be made available online to all users of IT resources, with cross references from the ITSD website.

#### Exceptions

- J. Guidance for requesting exceptions to or deviations from this directive is outlined in *AD 7.5A Establishing IT-Related Directives*.

### **Roles & Responsibilities**

#### **Chief Information Security Officer**

- A. Review this directive annually, at a minimum, for both consistency and accuracy
- B. Interpret and apply this directive under the direction of the Chief Information Officer (CIO) and/or the Chief Technology Officer (CTO), as appropriate
- C. Modify or amend this directive at any time pending formal review and approval as defined in *AD 7.5A Establishing IT-Related Directives*
- D. Provide adequate notice of any such modifications or amendments



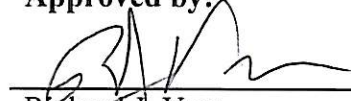
	<p>E. Ensure the current version of this directive is posted in a public location accessible to all authorized City personnel</p> <p>F. Review documented process for compliance</p>
<b><u>ITSD</u></b>	<p>A. Develop processes and procedures to describe how each topic is implemented in the COSA environment.</p>
<b><u>Business System Owners</u></b>	<p>A. Create and document the process they use to grant and manage user access and permissions (e.g., user accounts) to systems under their administration</p> <p>A. Identify personnel who shall have access to the system for which they are owners</p> <p>B. Identify the data that the systems maintain, store, or process</p> <p>C. Develop provisions for the timely termination of accounts</p> <p>D. Provide training regarding user responsibilities for complying with this directive</p>
<b><u>System Administrators</u></b>	<p>A. Identify personnel who shall have access to the system for which they are owners</p> <p>B. Identify the data that the systems maintain, store, or process</p> <p>C. Review accounts as defined by the business or system owner, no less than annually, for which they are responsible against lists/rosters of possible users</p>
<b><u>Departments</u></b>	<p>A. Responsible for any disciplinary action taken against employees who violate this directive</p>
<b><u>Human Resources</u></b>	<p>A. Provide guidance, as required, to City departments regarding appropriate disciplinary action to be taken against employees who violate this directive</p>
<b><u>Attachments</u></b>	
<b><u>N/A</u></b>	

Information and/or clarification may be obtained by contacting the Information Technology Services Department (ITSD) at 207-8301.

  
 \_\_\_\_\_  
 Hugh Miller  
 Information Technology Services Department Director / CTO

09/14/2009  
 \_\_\_\_\_  
 Date

Approved by:

  
Richard J. Varn  
Chief Information Officer (CIO)

09/16/09

Date

Approved by:

  
Sheryl Seutley  
City Manager

9-29-09

Date